Next Up Previous Contents
suivant: Exemple : accès POP **monter:** Tunnels avec Stunnel **précédent:** Tunnels avec Stunnel **Table des matières**

Stunnel

Stunnel est un programme qui permet de crypter les connexions TCP grâce aux librairies SSL (Secure Sockets Layer). Il peut être utilisé pour crypter des échanges d'informations pour des services qui ne sont pas sécurisés nativement, comme ceux que nous avons cité précédement. Pour utiliser stunnel, il est **obligatoire** d'avoir installé une librairie SSL du type OpenSSL ou SSLeay, puisqu'elles assurent le cryptage / décryptage pour stunnel.

Stunnel nécessite la création de certificats SSL (X509) pour fonctionner, ce qui permet au client et au serveur de s'identifier mutuellement de manière sûre (dans la mesure où elles font confiance à une autorité tierce). Il est possible de se passer de certificats sur la machine cliente, mais pour lancer un service stunnel, il faut obligatoirement disposer d'un certificat valide. L'option "noauth" permet de lancer stunnel en autorisant les connexions sans authenfication sur le serveur, et l'option -d passera le programme en démon. Ici, nous nous interesserons bien sûr plus à la mise en place d'un tunnel qu'à la génération de certificats, c'est pourquoi les commandes de génération des certificats ne seront pas explicitées.

- création d'une autorité de certification
- génération du certificat pour le service
- génération de certificats pour les clients (sauf si on ne fait pas d'authentification au niveau du serveur)

Note : A partir de la version 4.0 de Stunnel, la configuration des tunnels doit se faire à partir des fichiers de configuration associés au programme stunnel. Le principe reste exactement le même bien sûr, mais les commandes ne sont plus tout à fait les mêmes.

Next Up Previous Contents
suivant: Exemple : accès POP **monter:** Tunnels avec Stunnel **précédent:** Tunnels avec Stunnel **Table des matières**
root 2004-05-04